UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- x

UNITED STATES OF AMERICA :

- v. - : 15 Cr. 136 (RJS)

ERIC SALDARRIAGA, :

Defendant. :

- x

GOVERNMENT'S SENTENCING MEMORANDUM

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for the United States of America

Daniel S. Noble
Assistant United States Attorney
- Of Counsel -

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- x

UNITED STATES OF AMERICA :

- v. - : 15 Cr. 136 (RJS)

ERIC SALDARRIAGA, :

Defendant. :

- x

SENTENCING MEMORANDUM

The Government respectfully submits this memorandum in connection with the sentencing of defendant Eric Saldarriaga (the "defendant"), which is currently scheduled for June 26, 2015 at 2:00 p.m. In its Presentence Investigation Report ("PSR") dated May 28, 2015, the United States Probation Office ("Probation Office") correctly states that the applicable United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") range for the defendant is 0 to 6 months' imprisonment. For the reasons that follow, the Government respectfully submits that a sentence that includes a term of incarceration within the advisory Guidelines range would be sufficient, but not greater than necessary, to serve the legitimate purposes of sentencing set forth in Title 18, United States Code, Section 3553(a).

I. BACKGROUND

A. The Offense Conduct

At all relevant times, the defendant worked as a private investigator in New York City, including since at least July 2013 through his firm, Iona Research & Security Services, Inc.,

located in Queens. (PSR ¶ 6).[1] Between at least 2009 and March 2014, through certain services advertised on the internet (the "Hacking Services"), the defendant hired other individuals to hack into, *i.e.*, to gain unlawful and secret electronic access to, the e-mail accounts of almost 50 different individuals (collectively, the "Victims"). (PSR ¶¶ 2, 7). For certain victims, the defendant attempted to gain unlawful access to more than one email account. In total, the defendant hired the Hacking Services to attempt to hack into, and provide the defendant with unauthorized access to, at least 60 different e-mail accounts. (Id.)

More specifically, the defendant contacted the Hacking Services via e-mail to request the username and password for a particular Victim's e-mail account. In cases where the Hacking Services were able to obtain the username and password for the requested account, the Hacking Service would typically e-mail the defendant a screenshot of the inbox of the successfully hacked e-mail account and demand payment. The defendant then paid the Hacking Services, typically via an online payment system such as PayPal, to obtain the username and password for the Victim. (PSR ¶ 7). Having obtained the user credentials for the Victims' email accounts, the defendant then unlawfully accessed and reviewed the Victims' e-mail communications, sometimes for the purpose of furthering investigations on behalf of his paying clients, and sometimes to investigate individuals in which the defendant was interested for personal reasons. (Id.). The defendant earned approximately $5,000 from clients on whose behalf the defendant attempted to gain access to Victims' e-mail accounts.

[1] Although the Information to which the defendant pleaded guilty stated that the defendant was a "licensed private investigator," the defendant subsequently brought to the Government's attention that he never in fact obtained a private investigator license in New York State.

B. Procedural History

In connection with an investigation that was conducted by the Federal Bureau of Investigation ("FBI") Los Angeles Field Office, in October and December 2012, United States Magistrate Judges in the Central District of California authorized search warrants for e-mail accounts used by certain Hacking Services. Based on a subsequent review of the search warrant returns, the FBI learned that a particular e-mail account (the "Subject Account") had used the Hacking Services to attempt to obtain user credentials for the Victims' e-mail accounts. Through subsequent investigation, the FBI was able to identify the defendant as the user of the Subject Account.

On March 13, 2014, the FBI executed a search warrant at the defendant's residence in Queens, out of which the defendant had conducted his private investigation work. The same day, FBI agents interviewed the defendant. During the interview, the defendant told the agents that he was a private investigator and owned the firm Iona Research & Security Services. After the agents confronted the defendant about the Subject Account, the defendant stated that he was familiar with various Hacking Services and had obtained passwords for e-mail accounts for payment. The defendant was cooperative and provided the agents with other email accounts that he used for his investigative work and the passwords for various electronic devices that the FBI seized.

On April 1, 2014, the defendant participated in a proffer session with FBI agents and a Government attorney. During the proffer, the defendant provided the Government with information concerning his use of the Hacking Services to obtain usernames and passwords for the Victims' e-mail accounts. The defendant told the Government that approximately 70 to 80 percent of the e-mail accounts to which he attempted to obtain access were hacked for personal

reasons; the remainder were hacked to further his investigative work on behalf of clients. Following his initial proffer, the defendant attempted to cooperate, including by making recorded phone calls with the main client who had hired the defendant to hack into certain individuals' e-mail accounts. The defendant's attempts at cooperation, however, did not yield sufficient evidence to charge any other individuals. Because the defendant was not in a position to provide substantial assistance, the Government did not offer him a cooperation agreement.

On March 6, 2015, the defendant waived indictment and pleaded guilty to information 15 Cr. 136 (RJS) (the "Information"), pursuant to a plea agreement with the Government. (PSR ¶ 4). The Information charged the defendant with one count of conspiracy to commit computer hacking, in violation of 18 U.S.C. § 1030(b). (PSR ¶ 2). In the plea agreement, the parties stipulated that the applicable Guidelines range was 0 to 6 months' imprisonment. (PSR ¶ 4).

C. The Guidelines Calculation

Pursuant to U.S.S.G. §§ 2X1.1 and 2B1.1(a), the base offense level for Count One is six. (PSR ¶ 13). A two-level enhancement applies because the offense involved more than 10 but less than 50 victims, pursuant to U.S.S.G. § 2B1.1(b)(2)(A)(i). (PSR ¶ 14). Another two-level enhancement applies because the defendant was convicted of an offense under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information, pursuant to U.S.S.G. § 2B1.1(b)(17)(A). (PSR ¶ 15). Finally, pursuant to U.S.S.G. § 3E1.1(a), a two-level reduction is warranted for the defendant's demonstration of acceptance of responsibility. (PSR ¶ 21). Thus, the defendant's total adjusted offense level is 8. (PSR ¶ 22). Because the defendant has no known prior criminal convictions, he is in Criminal History Category I, which yields a Guidelines range of 0 to 6 months' imprisonment.

The Probation Office has recommended a sentence of three years' probation to include 6 months' home confinement and a fine of $1,000. (Sentencing Recommendation, PSR at 18).

II. APPLICABLE LAW

The United States Sentencing Guidelines still provide strong guidance to the Court following United States v. Booker, 543 U.S. 220 (2005), and United States v. Crosby, 397 F.3d 103 (2d Cir. 2005). Although Booker held that the Guidelines are no longer mandatory, it also held that the Guidelines remain in place and that district courts must "consult" the Guidelines and "take them into account" when sentencing. Booker, 543 U.S. at 264. As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range" — that "should be the starting point and the initial benchmark." Gall v. United States, 552 U.S. 38, 49 (2007).

After that calculation, however, a sentencing judge must consider seven factors outlined in 18 U.S.C. § 3553(a): "the nature and circumstances of the offense and the history and characteristics of the defendant," 18 U.S.C. § 3553(a)(1); the four legitimate purposes of sentencing, see id. § 3553(a)(2); "the kinds of sentences available," id. § 3553(a)(3); the Guidelines range itself, see id. § 3553(a)(4); any relevant policy statement by the Sentencing Commission, see id. § 3553(a)(5); "the need to avoid unwarranted sentence disparities among defendants," id. § 3553(a)(6); and "the need to provide restitution to any victims," id. § 3553(a)(7). See Gall, 552 U.S. at 50 & n.6.

In determining the appropriate sentence, Section 3553(a) directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;

(B) to afford adequate deterrence to criminal conduct;

(C) to protect the public from further crimes of the defendant; and

(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2). To the extent District Court imposes a sentence outside the range recommended by the Guidelines, the Court must "consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance." United States v. Cavera, 550 F.3d 180, 189 (2d Cir. 2008) (*en banc*) (internal quotation marks omitted).

III. DISCUSSION

In light of the need to impose a sentence upon the defendant that reflects the seriousness of the offense, promotes respect for the law, and provides just punishment, and that has a sufficiently strong deterrent effect for this defendant and others, the Government respectfully submits that a sentence that includes a period of incarceration within the advisory Guidelines range of 0 to 6 months' imprisonment is appropriate.

First, a term of incarceration is necessary to reflect the serious nature of the crime, to promote respect for the law, and to provide just punishment. See 18 U.S.C. § 3553(a)(2)(A). Over the course of several years, the defendant attempted to gain unlawful access to nearly 50 different Victims' e-mail accounts. In some cases, the defendant acted on behalf of clients who were paying him to investigate the Victims; in other cases the defendant's hacking was motivated by the defendant's own personal interest in the content of the Victims' e-mail accounts. In either case, the defendant's conduct represented an egregious violation of the Victims' privacy rights. It goes without saying that e-mail accounts oftentimes contain

individuals' most personal communications, including correspondence about one's personal relationships, finances, business affairs, and medical information. Through his e-mail hacking activities, the defendant repeatedly intruded into these intimate discussions.

Moreover, the defendant's involvement in criminal activity was not some momentary lapse in judgment or isolated to a single or even a few e-mail accounts. To the contrary, the defendant used Hacking Services to try to gain access to approximately 60 e-mail accounts over several years. Furthermore, even though the defendant was not was not properly licensed as a private investigator in New York State, he nevertheless held himself out as such. As someone working in that professional capacity, the defendant should have known better. Instead, the defendant flouted the laws to cut corners to further investigations on behalf of his clients, or to satisfy his own personal interest in the contents of the Victims' e-mail accounts. Accordingly, the defendant is wholly deserving of a term of imprisonment within the applicable Guidelines range. Such a sentence would reflect the seriousness of his conduct, promote respect for the law, and provide just punishment.

In addition, one of the most important factors that this Court must consider in imposing a sentence under Section 3553(a) is the need for the sentence to "afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(B). Given the inherent difficulties in detecting and pursuing cybercrime, and the defendant's proven potential for engaging in illegal acts to further his own business and personal interests, general and specific deterrence are of great importance here. Computer hacking is becoming an ever more prevalent threat in our society. Using inexpensive and easy-to-use hacking tools, such as the online Hacking Services used by the defendant, cyber criminals can obtain access to others' computers and e-mail accounts. With such unfettered access, cybercriminals can steal the victims' personal and financial information,

spy on them, and gain access to their most intimate communications. Furthermore, given the anonymity of the internet and the proliferation of tools available to cyber criminals to evade law enforcement, significant penalties are necessary to send a message that hacking and other types of cybercrime will not go unpunished. Unlike defendants in a gun or drug case, who often act without reflection, there is reason to believe that individuals who engage in hacking and other forms of cybercrime can be deterred by a substantial threat of penalties. Their actions are calculated. They choose to engage in such crime because they believe that the potential for significant benefits outweighs the risk that they will be caught and punished. General deterrence is achieved by sending a message that such outrageous invasions of privacy – like the defendant's hacking of the Victims' e-mail accounts in this case – will result in real penalties. For this reason, a sentence within the advisory Guidelines range would be appropriate to deter this defendant and others who believe they can fly under the radar of law enforcement and profit from computer hacking and other cybercrime.

IV. CONCLUSION

For the foregoing reasons, the Government respectfully submits that a sentence within the advisory Guidelines range of 0 to 6 months' imprisonment for Eric Saldarriaga would be sufficient, but not greater than necessary, to serve the legitimate purposes of sentencing. The Government further requests that the Court order forfeiture in the amount of $5,000.00. The Government will provide a proposed forfeiture order for the Court's consideration at sentencing.

Dated: June 22, 2015
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney
Southern District of New York

By: _____/s/_____
Daniel S. Noble
Assistant United States Attorney
(212) 637-2239

AFFIRMATION OF SERVICE

The undersigned attorney, duly authorized to represent the United States before this Court, hereby certifies that on the date below, he served or caused to be served the following document(s) in the manner indicated:

GOVERNMENT'S SENTENCING MEMORANDUM

Service via electronic mail to:

Peter Brill, Esq.
Counsel for Peter Brill

Dated: June 22, 2015

_____/s/_____
Daniel S. Noble
Assistant United States Attorney
(212) 637-2239